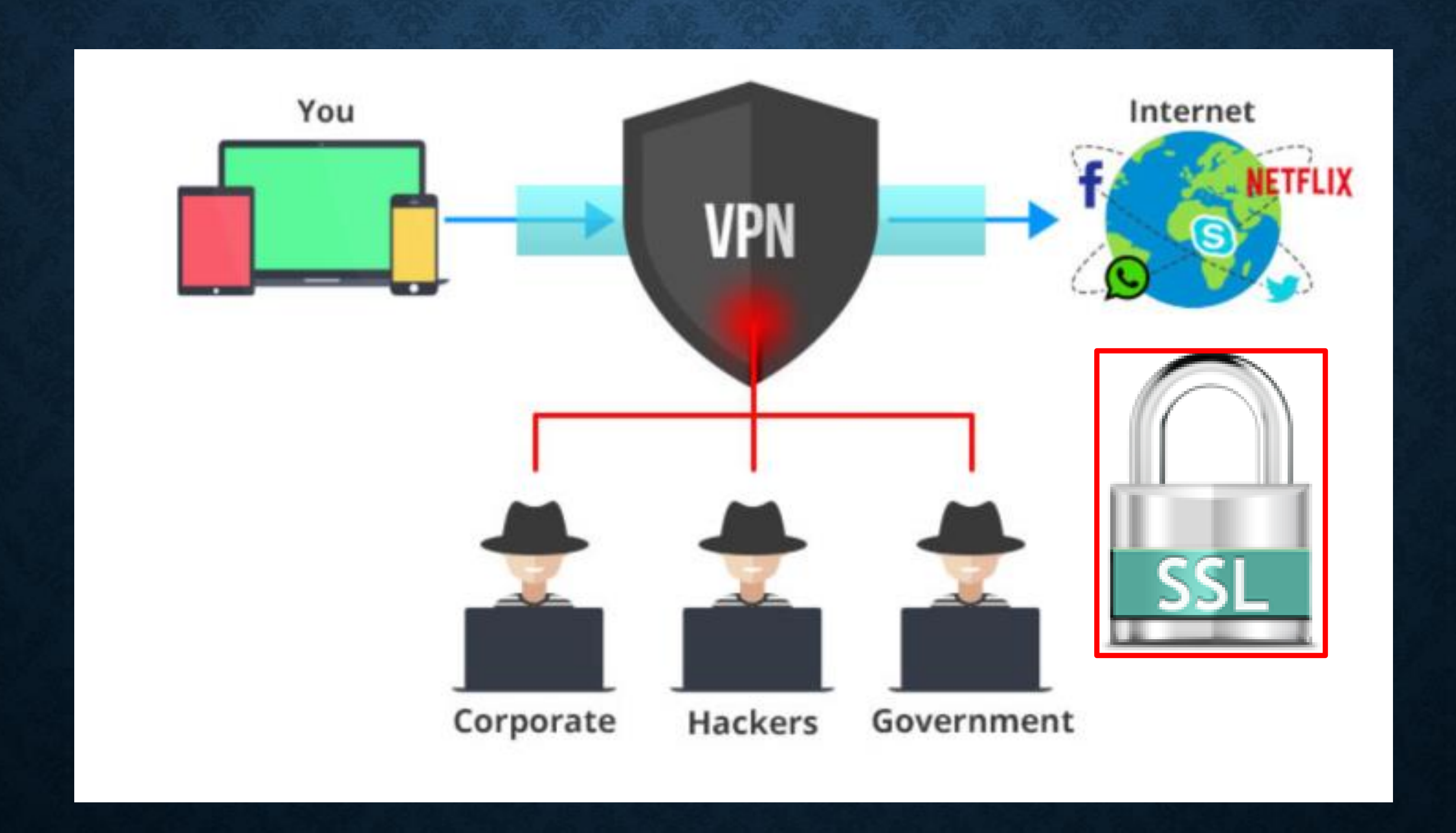
# SSL ET VPN



You
VPN
Internet
NETFLIX
SSL
Corporate
Hackers
Government

# 1- LE PROTOCOLE SSL

- **SSL (Secure Sockets Layer)** est un protocole utilisé pour **chiffer** et **authentifier** les données envoyées entre une application (comme votre navigateur) et un serveur web.
- 1re avantage de SSL est le **chiffrement**. Chaque fois que vous entrez des informations sur votre site web, ces données seront sécurisés pour assurer une  protection point à point.
- 2ème avantage est **l'intégrité des données** pendant le transport. Ceci garantit que les données qui sont envoyées sont reçues sans aucune modification ou altération malveillante.
- 3ème avantage est **l'authentification**. Une connexion SSL en bon état de fonctionnement garantit que les données sont envoyées et reçues par le bon serveur, plutôt que par un « homme au milieu » malveillant. Il empêche les acteurs malveillants de se faire passer pour un site à tort.

0100
ENCRYPTED AND JUMBLED
11011
Can't understand data!!!

# 2- LES CERTIFICATS SSL (X-509)

- Le protocole SSL utilise le **chiffrement asymétrique** (qui est basé sur une paire de clés **privée** et **publique**) pour **chiffrer** et **signer** les données.
- L'administrateur du **serveur Web** doit **générer ces deux clés** sous forme des fichiers:
  - Un 1re fichier caché qui contient la **clé privée**.
  - Un 2ème fichier texte codé par cette clé privée et qui comprend la **clé publique** et d'autres informations (comme le nom du site web , organisation, adresse e-mail, etc.). Ce fichier consiste d'une demande qui sera envoyé à une **Autorité de certification**.
- Une **Autorité de certification**, est une entreprise ou une organisation qui agit pour valider l'identité des entités (telles que les sites Web, les adresses e-mail, les entreprises ou les particuliers) et les lier à des clés cryptographiques par la publication de documents électroniques appelés **certificats numériques X-509**.
- Une fois le certificat est approuvé, il est envoyé au serveur Web pour l'utiliser sur le site web.

# 2- LES CERTIFICATS SSL

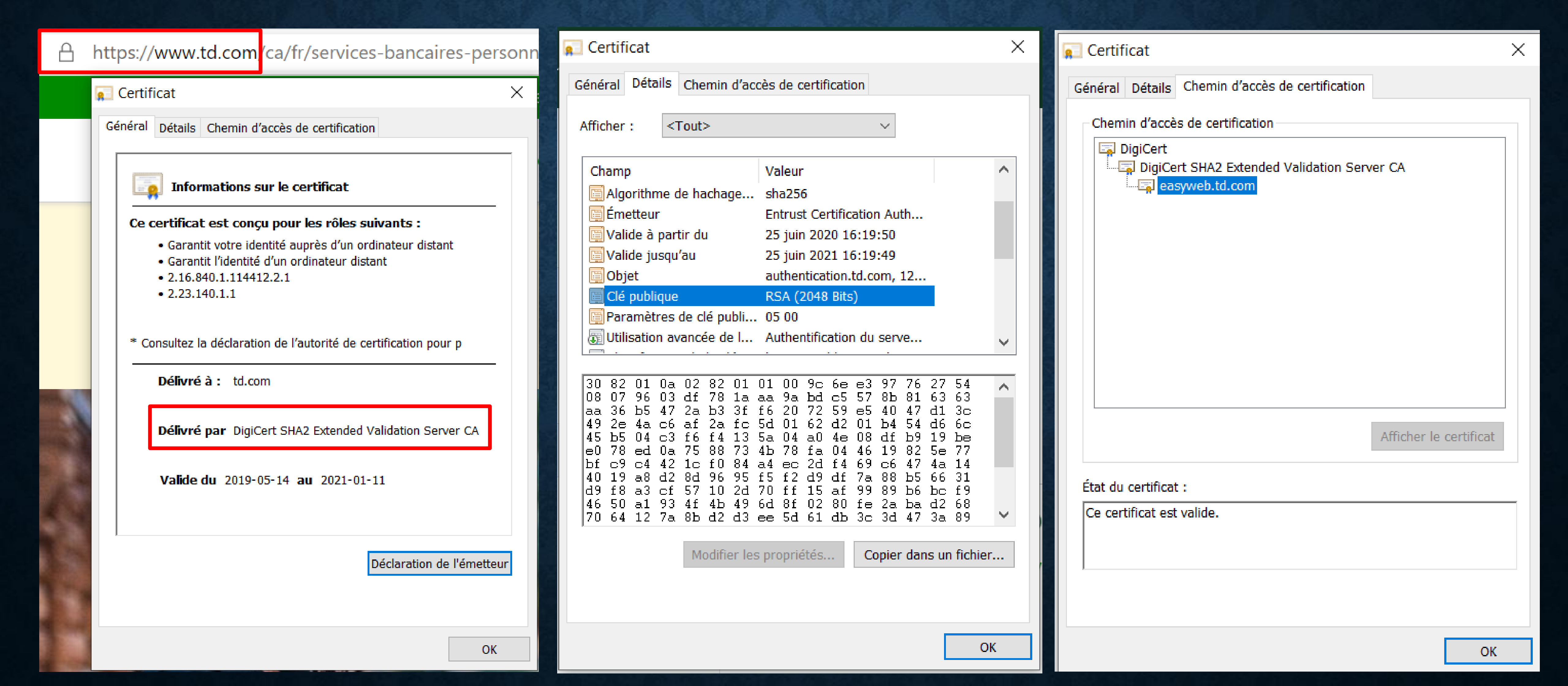
- Chaque serveur web sur Internet qui utilise HTTPS doit avoir une **certificat électronique SSL** fournie par une **autorité de certificat approuvée** sur Internet, exemple:
  - Entrust;
  - GoDaddy;
  - DigiCert;
  - Geotrust.




- Chaque certificat délivré à un serveur Web, doit contenir les informations suivantes:
  - le nom et le pays du propriétaire du certificat;
  - sa date de validité;
  - le système cryptographique associé;
  - la clé publique associée;
  - la signature de l'autorité de certification, qui doit garantir à la fois la justesse des informations du certificat, et leur origine.

# 2- LES CERTIFICATS SSL

- Exemple d'un **certificat électronique X-509 (SLL)** utilisé sur le site **HTTPS** de la banque TD:



# 3.1- ÉTAPES DE LA CONNEXION SSL - AUTHENTIFICATION DU SERVEUR

Amazon.ca: Low Prices – Fast Shi

amazon.ca

Applications TD Jard RBC Cruz MAJ PDA Cer

amazon.ca prime Deliver to Antoine Laval H7X 1S8 All

All Best Sellers Prime Antoine's Store Registry Deals Store

**1** Google chrome envoie une demande de connexion au serveur **amazon.ca**

**2** Serveur Amazon envoie **son certificat SSL** qui contient sa **clé publique** et **son empreinte** (créé par SHA-256 **en utilisant sa clé privé**).

Serveur Amazon

Certificat

Général | Détails | Chemin d'accès de certification

Chemin d'accès de certification

- DigiCert Global Root G2
  - DigiCert Global CA G2
    - www.amazon.ca

Afficher le certificat

État du certificat :

Ce certificat est valide.

OK

Certificat

Général | Détails | Chemin d'accès de certification

**Informations sur le certificat**

**Ce certificat est conçu pour les rôles suivants :**

- Garantit votre identité auprès d'un ordinateur distant
- Garantit l'identité d'un ordinateur distant
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

* Consultez la déclaration de l'autorité de certification pour p

**Délivré à :** www.amazon.ca

**Délivré par** DigiCert Global CA G2

**Valide du** 2020-07-12 **au** 2021-06-21

Déclaration de l'émetteur

OK

**Clé publique** stockée dans le certificat SSL

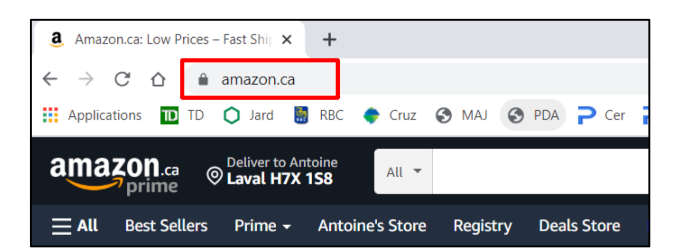

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmbvtPODy32rRJZYRQ
n/Fqr7rXanneZjVOMyPm38zCEckJe5o
25EPeobvf2nA38C7j/gEbPhRfOaP6FJ7G
Pbonzn92C8nigfhls4ytXHU0HeJH7IU
ioNtEoZ88LpQ0L9jRjnfmc1jqfLiTj4Tk
fU8pdk0aJBtOUgIp5GzbtUyMg01Ia2C
i3+wjwuhHNENUfWR0rYZH97vRmYAK8cLr
FYUy2TV24OqxBewSJdEjThnsjiBAFP1
rDsdDa/8JPfz0yXFUyTx2FTrdgzSbcEts
xx5M89OHrJk52Cb2TV8B7Mzj3n9aw5k
5HId0q6TK1HCVuEimt80r7/8iA


**Clé privée** reste caché sur le serveur

**3** Le client vérifie le certificat auprès de **l'autorité de certification** mentionné dans le certificat du serveur. Ex: **DigiCert Global.**



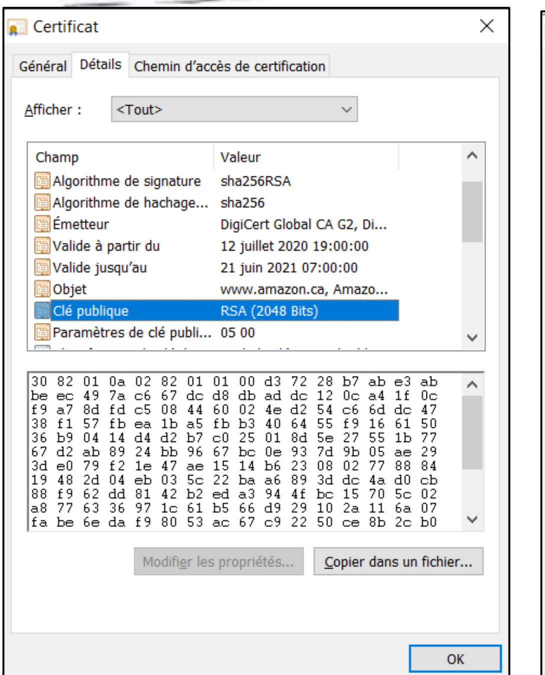
# 3.2- ÉTAPES DE LA CONNEXION SSL - INTÉGRITÉ DES DONNÉES

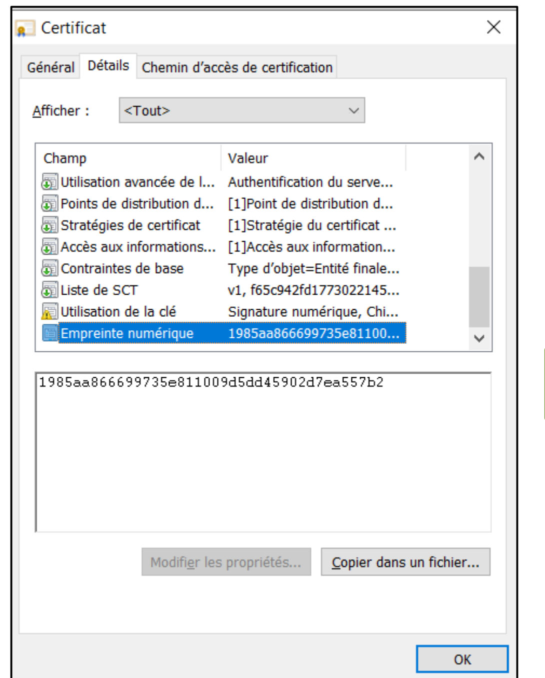





5

Google chrome fait le même calcul de **hachage,** en **utilisant la clé publique du serveur**, génère **une nouvelle empreinte** et la compare avec celle du serveur pour s'assurer que **les données n'étaient pas modifiés** par un tiers en transit.

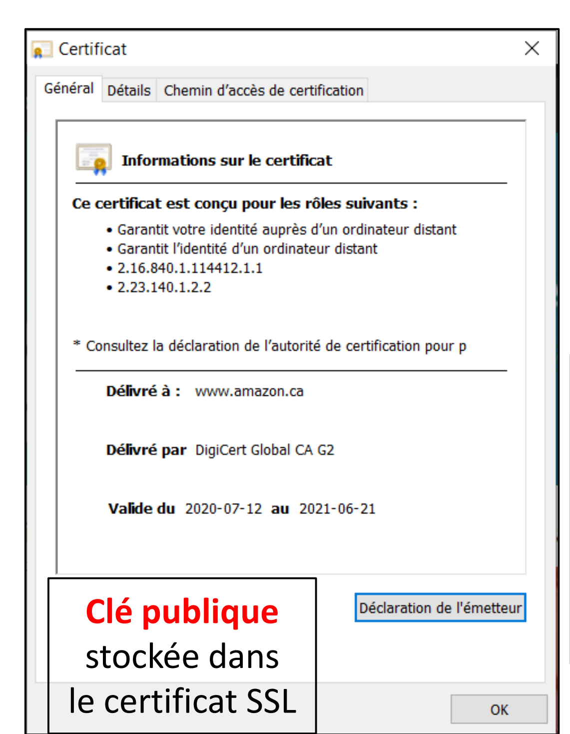



4

Si le certificat est reconnu par l'autorité de certification.




**Clé publique** stockée dans le certificat SSL

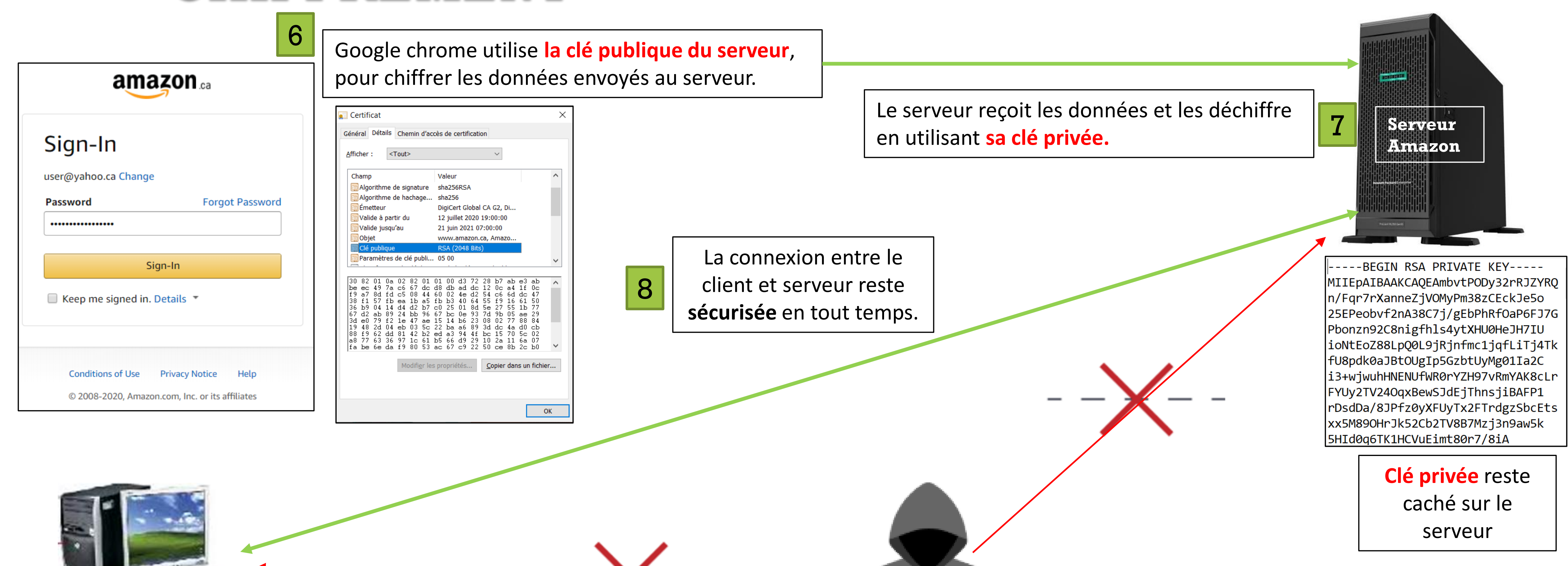




-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmbvtPODy32rRJZYRQ
n/Fqr7rXanneZjVOMyPm38zCEckJe5o
25EPeobvf2nA38C7j/gEbPhRfOaP6FJ7G
Pbonzn92C8nigfhls4ytXHU0HeJH7IU
ioNtEoZ88LpQ0L9jRjnfmc1jqfLiTj4Tk
fU8pdk0aJBtOUgIp5GzbtUyMg01Ia2C
i3+wjwuhHNENUfWR0rYZH97vRmYAK8cLr
FYUy2TV24OqxBewSJdEjThnsjiBAFP1
rDsdDa/8JPfz0yXFUyTx2FTrdgzSbcEts
xx5M89OHrJk52Cb2TV8B7Mzj3n9aw5k
5HId0q6TK1HCVuEimt80r7/8iA


**Clé privée** reste caché sur le serveur

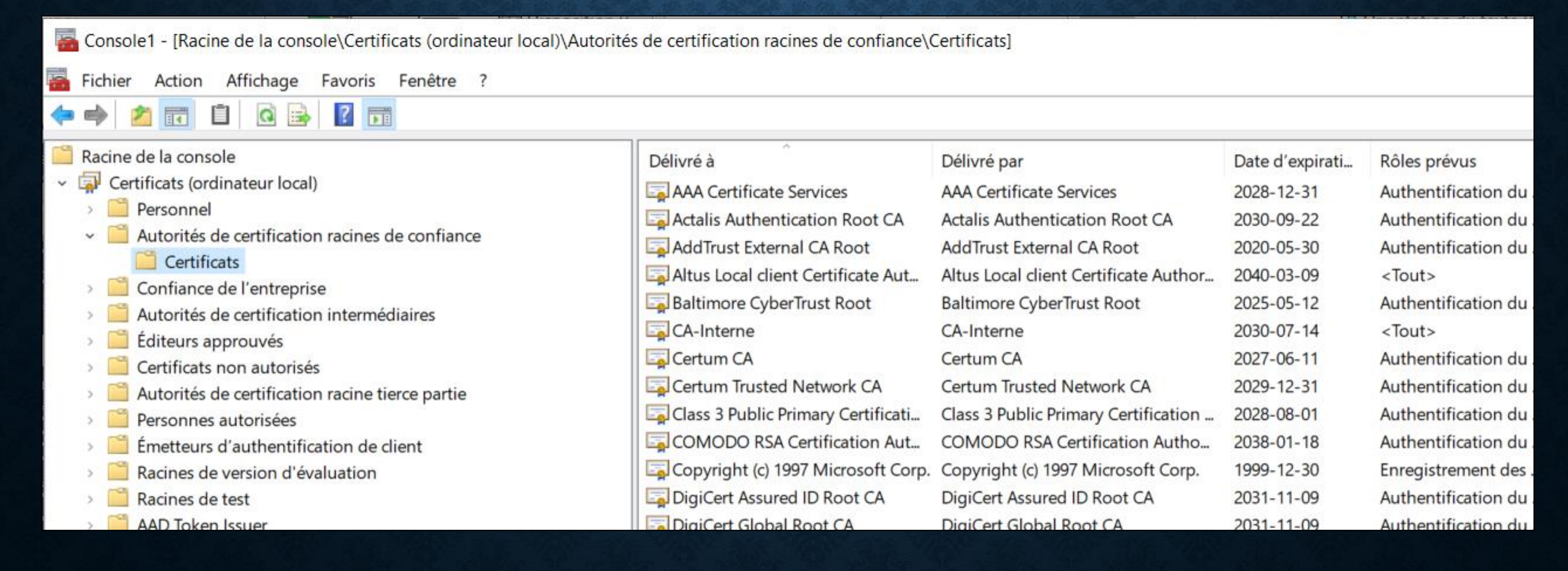
# 3.3- ÉTAPES DE LA CONNEXION SSL - CHIFFREMENT




Man-in-the-Middle

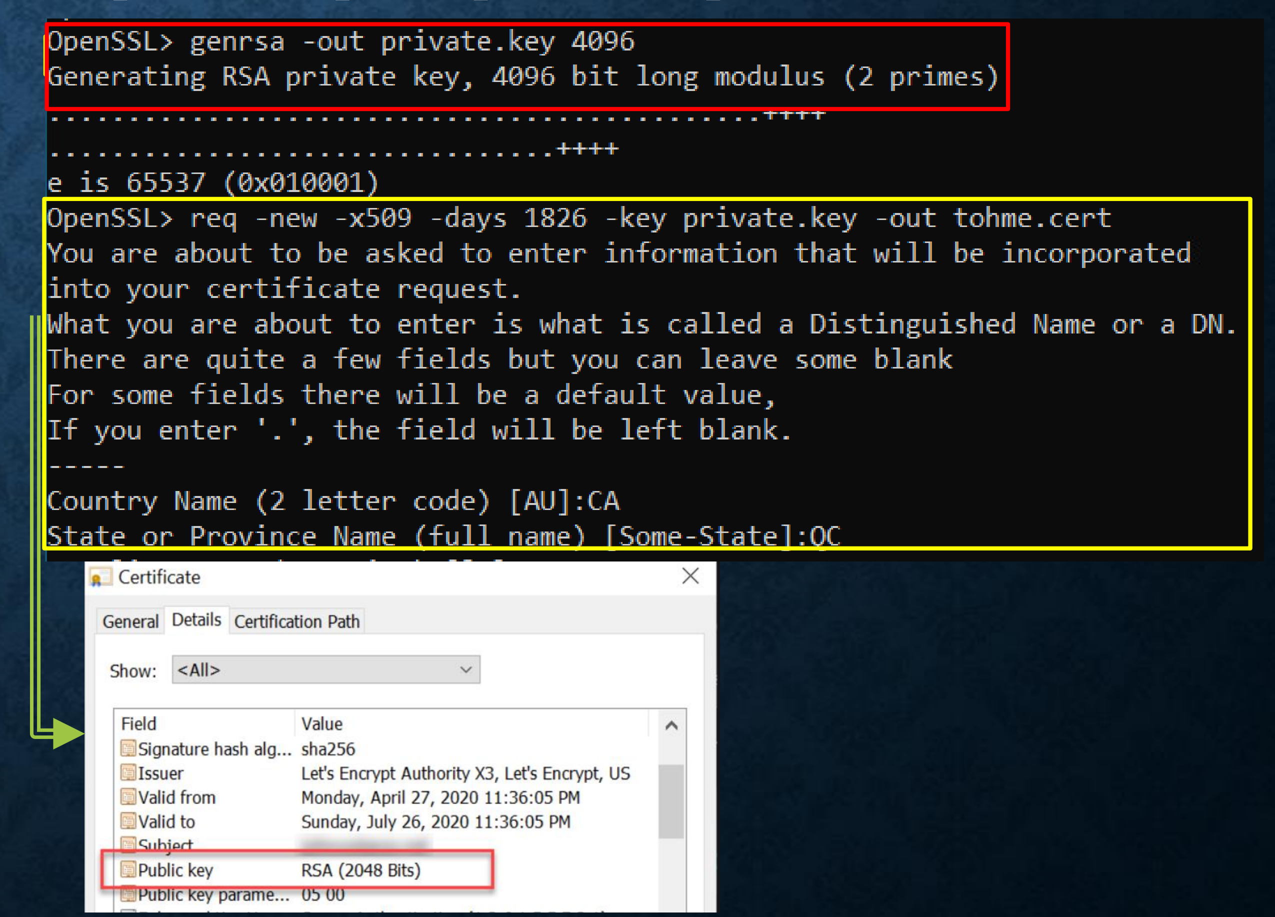
# 4- MAGASIN DE CERTIFICAT – WINDOWS 10

- Tous les systèmes d'exploitation vient avec une base de données de tous les **autorités de certificat approuvées.**
- Vous pouvez utilisez l'outil de Windows 10 **MMC** pour afficher ces certificats.



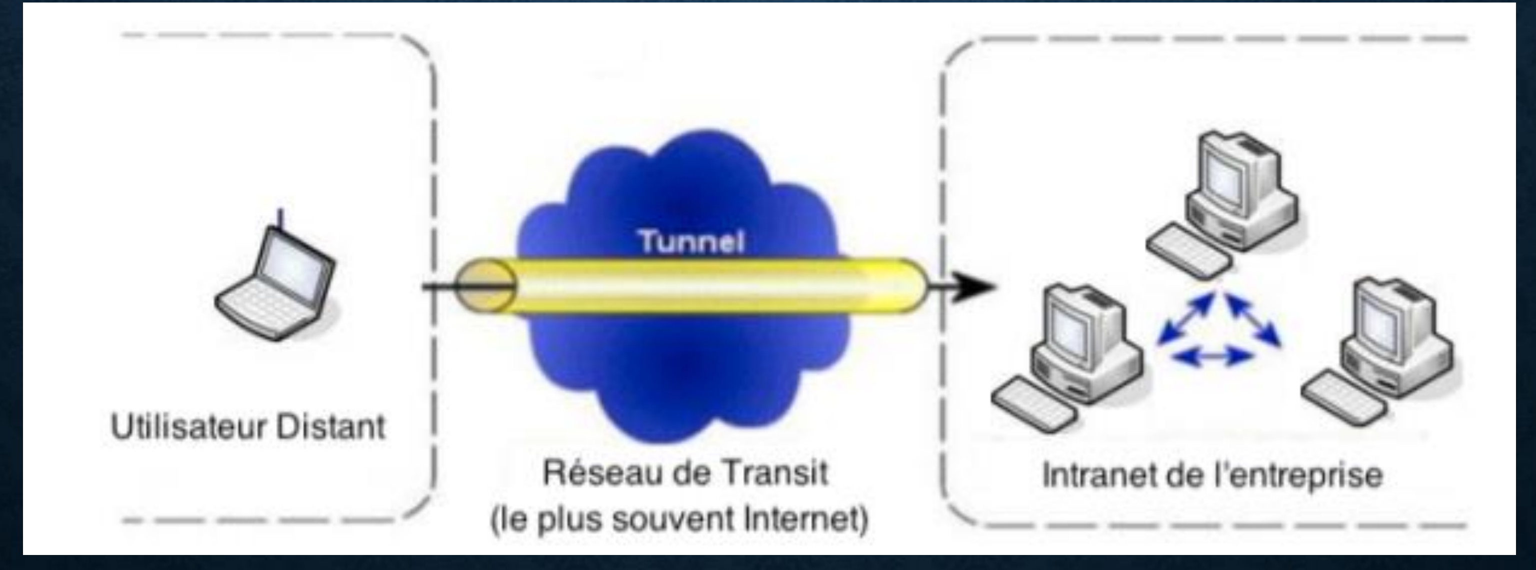
# 5- CRÉATION DES CERTIFICATS SSL AUTONOME

- Vous pouvez créer **votre propre certificat SSL**, sans utiliser un autorité de certification.
- Une fois créé, vous pouvez l'utiliser pour chiffrer et signer des données.
- Pour le faire, vous devez générer un jeu de clés privée et publique, ainsi qu'un certificat SSL contenant la clé publique.
- Il existe de nombreux moyens de générer ces paires de clé publique et privée, mais l'outil **OpenSSL** reste l'un des plus populaires.
- OpenSSL utilise **l'algorithme RSA** pour générer la **clé privée**, puis à partir de cette clé, il créé un **certificat qui contient la clé publique.**
- **Voir Lab 10 – Création des certificats SSL.**



# 6- VPN (VIRTUAL PRIVATE NETWORK)

- Les **VPN (Virtual Private Network)** sont des réseaux virtuels privés qui permettent la connexion **entre deux réseaux à travers un tunnel sécurisé.**
- C'est à dire que les données qui transitent par ce tunnel sont **chiffrées** afin notamment de protéger contre les attaques MIM (Man in the Middle).
- L'exemple type est une connexion VPN entre un télétravailleur et l'intranet de son entreprise.

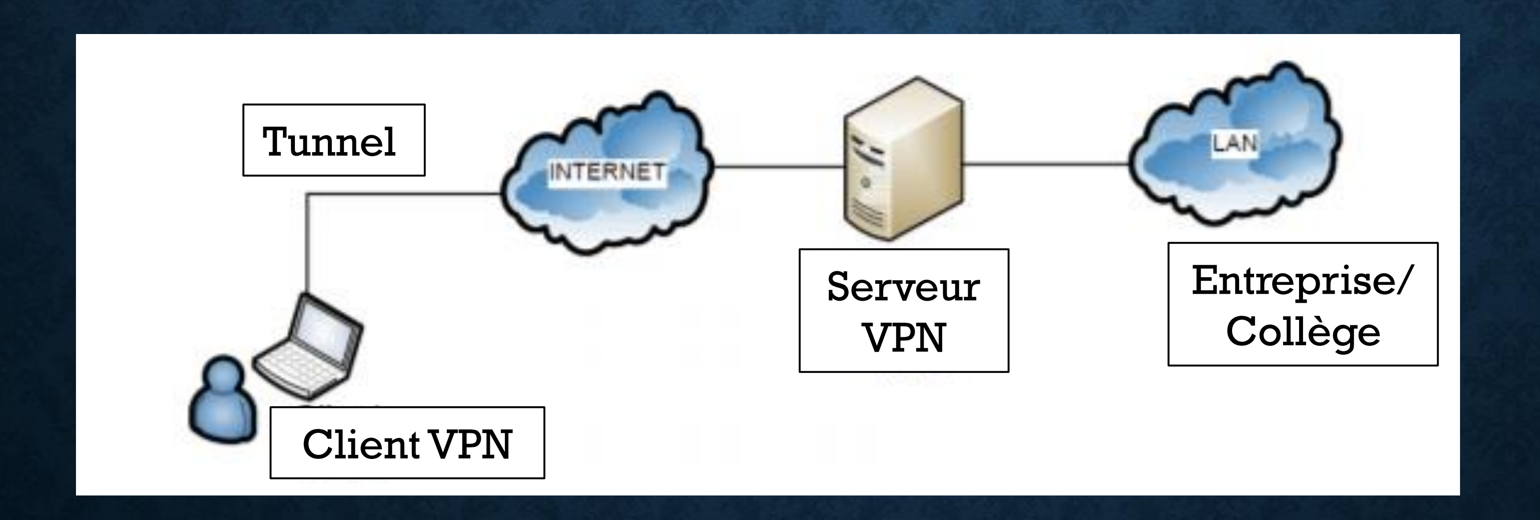


# 8- LES FONCTIONNALITÉS DU VPN

- Un système de VPN sécurisé doit pouvoir mettre en œuvre les fonctionnalités suivantes :
  - Authentification d'utilisateur : Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel.
  - Gestion d'adresses : Chaque client sur le réseau dispose d'une adresse IP privée et confidentielle.
  - Cryptage des données : Lors de leur transport sur le réseau public les données doivent être protégées par un cryptage efficace.
  - Gestion de clés : Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

# 7- LES ÉLÉMENTS DU VPN

- Dans le cas d'une connexion VPN d'accès distant, plusieurs éléments sont nécessaires :
  - Le serveur VPN : situé dans l'entreprise, qui accepte les connexions VPN des clients.
  - Le client VPN : distant, qui se connecte au serveur VPN.
  - Le tunnel : la connexion dans laquelle les données sont chiffrées.



# 7.1- LES ÉLÉMENTS DU VPN – SERVEUR VPN

- Un serveur VPN peut être un **équipement matériel (Hardware)** comme un routeur ou un pare-feu. https://www.virtuallocation.com/vpn/vpn-hardware.html





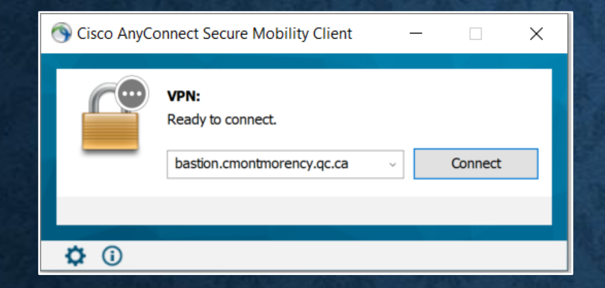



- Il peut aussi être **un logiciel (software)** installé sur un serveur.
- Microsoft, UNIX, AS400 et Linux permettent d'utiliser des services VPN.



# 7.2- LES ÉLÉMENTS DU VPN – CLIENT VPN

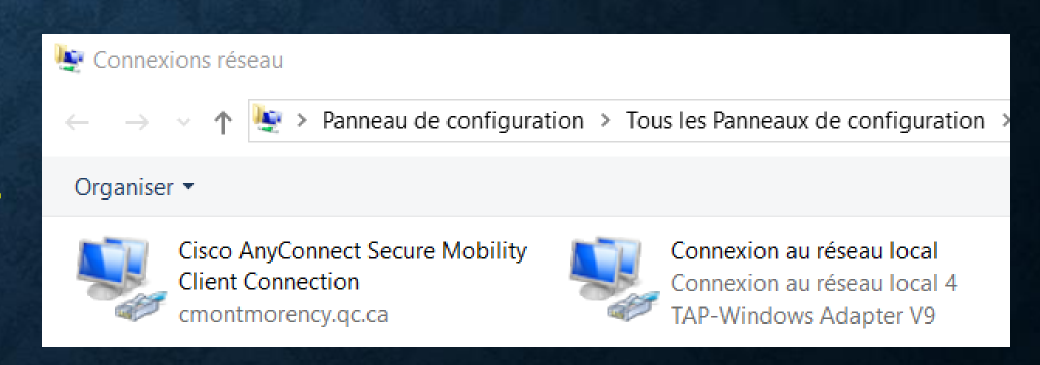
- Quelque soit le serveur est matériel ou logiciel, le client est toujours **un logiciel installé sur l'ordinateur** de l'utilisateur.
- Il existe de multiples clients, comme par exemple Cisco AnyConnect et OpenVPN.





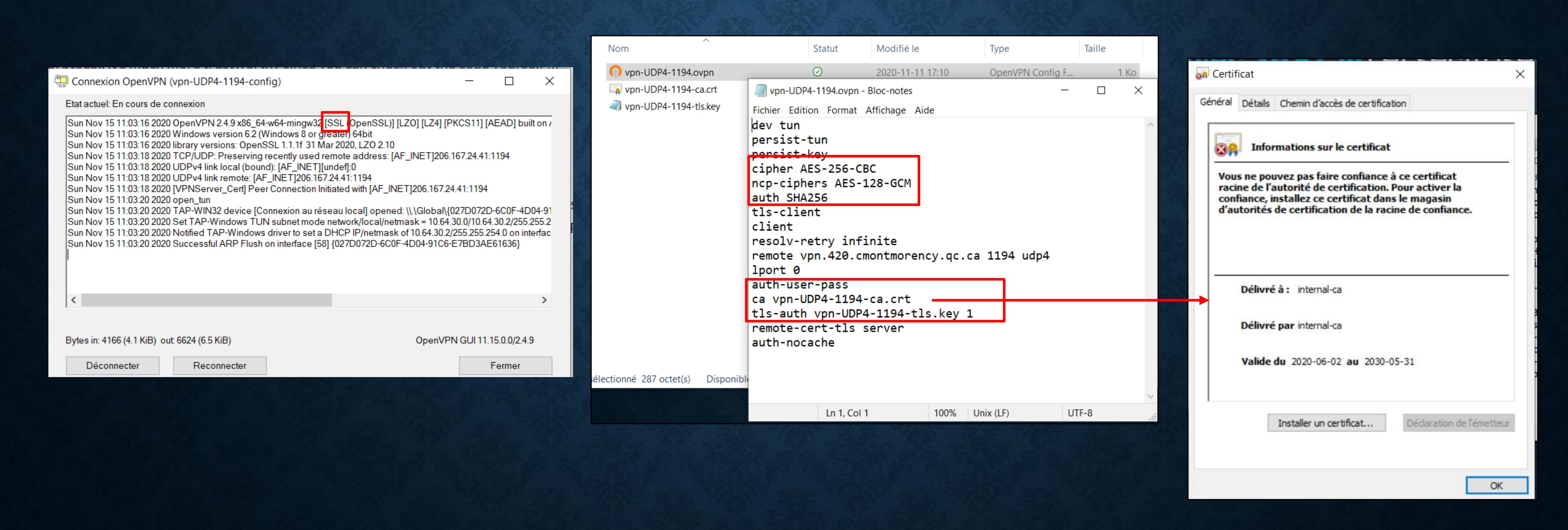


- À l'installation du client, une **carte réseau virtuelle** est créée.
- Cette carte réseau reçoit **une adresse IP** envoyée par le serveur VPN, quand la connexion est établie.
- Exemple: Connectez-vous avec OpenVPN du collège puis exécutez **ipgonfig /all**



# 7.3- LES ÉLÉMENTS DU VPN – TUNNEL VPN

- Pour créer ce tunnel sécurisé, le client utilise le **protocole SSL** pour initier la connexion (**Authentification avec SHA-256**) et sécurisé les données (**Chiffrement avec AES-256**).



# 8- FOURNISSEURS DE VPN "GRAND PUBLIC"

- Il existe des services VPN grands publics (NordVPN, ExpressVPN, CyberGhost, ProtonVPN, ...).
- Ces derniers misent sur **la sécurité et l'anonymisation** pour vendre des solutions clés en main.
    - L'internaute s'inscrit et paye un abonnement à un fournisseur VPN.
    - Ensuite il installe le client sur son ordinateur ou smartphone Android/IOS.
    - Puis il authentification avec son compte.
    - A partir de là, il choisit les serveurs disponibles auxquels se connecter. Généralement, on choisit le serveur selon la localisation géographique.
    - La connexion au serveur s'établit et tout le trafic internet passe alors par le VPN.
    - Les services internet voient alors l'IP du serveur VPN et plus celle la connexion internet et du fournisseur d'accès.

> L'idée des VPN grands publics est donc de connecter votre appareil (PC, Smartphone) à un serveur VPN et de rediriger tout votre trafic internet dessus.
> Il sert donc d'intermédiaire pour se connecter aux services internet finaux (Youtube, Netflix, site internet, jeux en ligne, etc).
> Ainsi ces derniers voient l'adresse IP du serveur VPN et non celle de votre fournisseur d'accès.